

サイバーセキュリティと データ管理監督法制の体系整理

～中国の安全保障貿易管理に関する制度情報
専門家による政策解説～

2021年11月

日本貿易振興機構（ジェトロ）

北京事務所

海外調査部

【免責条項】

本レポートは、北京市環球法律事務所に委託し、作成したものです。
本レポートで提供している情報は、ご利用される方のご判断・責任においてご使用下さい。ジェトロでは、できるだけ正確な情報の提供を心掛けておりますが、本レポートで提供した内容に関連して、ご利用される方が不利益等を被る事態が生じたとしても、ジェトロおよび執筆者は一切の責任を負いかねますので、ご了承下さい。

中国では2017年より情報セキュリティ分野の基本法である「中華人民共和国サイバーセキュリティ法」（以下、「サイバーセキュリティ法」）が施行されていますが、2021年に入って、データの国内保管や情報の内部統制を目的とした「中華人民共和国データセキュリティ法」（以下、「データセキュリティ法」）および「中華人民共和国個人情報保護法」（以下、「個人情報保護法」）が相次いで施行され、同分野における規制はより厳格化しています。

1. サイバーセキュリティおよびデータに関連する法令

(1) 基本法

上述した「サイバーセキュリティ法」「データセキュリティ法」「個人情報保護法」のほか、「中華人民共和国民法典」（以下、「民法典」）、「中華人民共和国刑法」（以下、「刑法」）等にもサイバーセキュリティおよびデータに関連する規定があります。主な内容は以下のとおりです。

	法令名	サイバーセキュリティおよびデータに関連する主な内容
1.	民法典	第4編「人格権」第6章「プライバシー権および個人情報保護」で、個人情報の取り扱い、関連の権利・義務について定めています。
2.	刑法	サイバーセキュリティおよびデータに関連する罪名を定めています。
3.	サイバーセキュリティ法	ネットワーク運用上のセキュリティと、ネットワーク情報のセキュリティについて定めています。また、ネットワーク・データセキュリティ上のキーワードとされる「重要情報インフラ」および「重要情報インフラ運営者」という新たな用語が同法にて初めて登場しました。
4.	個人情報保護法	個人情報の取り扱いにおけるセキュリティ要件および個人情報主体の権利保護等について定めています。また、個人情報・機微な個人情報・未成年者の個人情報およびそれらの取り扱いに関する要件、個人情報の越境移転等についても定めています。
5.	データセキュリティ法	「データ」の定義について「電子的またはその他の方式による情報に対するあらゆる記録」と定めています（すなわち、「個人情報保護法」における個人情報および「サイバーセキュリティ法」におけるネットワーク情報は「データ」に含まれます）。また、データ分類・等級付け保護制度および重要データ・国家中核データ、データ国外移転のルール等を定めています。

(2) 特定分野の関連法令

基本法のほか、特定分野の関連法令の整備も、国務院、国家インターネット情報弁公室等の関係政府機関により活発に行われています。主な分野、法令名（大部分は法令として成立していない草案段階のものです）ならびにその適用対象および内容については以下のとおりです。

	分野	法令名	適用対象および内容
1.	サイバーセキュリティ等級保護 （「サイバーセキュリティ法」第21条に基づく）	サイバーセキュリティ等級保護条例（意見募集稿）（公安部、2018年6月27日公開）	対象：ネットワーク運営者 内容：ネットワーク等級付け・届け出、等級付け保護等の義務の実行
2.	重要情報インフラ運営者（「サイバーセキュリティ法」第31～39条に基づく）	重要情報インフラセキュリティ保護条例（国务院、2021年9月1日施行）	対象：重要情報インフラ運営者 内容：サイバーセキュリティ保護、検査・評価、重要情報及び個人情報の国内保管等の義務（重要情報インフラの認定）
3.	データ域外移転規制（「サイバーセキュリティ法」第37条、「データセキュリティ法」第31条、第36条、「個人情報保護法」第38～41条に基づく）	個人情報域外移転安全評価弁法（意見募集稿）（国家インターネット情報弁公室、2019年6月13日公開） 個人情報および重要データ域外移転安全評価弁法（意見募集稿）（国家インターネット情報弁公室、2017年4月11日公開） データ域外移転安全評価弁法（意見募集稿）（国家インターネット情報弁公室、2021年10月29日公開）	対象：重要データ、個人情報を扱う重要情報インフラ運営者と非重要情報インフラ運営者 内容：自己評価、安全評価、標準契約締結等の義務
4.	サイバーセキュリティ審査（「サイバーセキュリティ法」第35条に基づく）	サイバーセキュリティ審査弁法（国家インターネット情報弁公室、国家発展改革委員会、工業情報化部、公安部、国家安全部、財政部、商務部、中国人民銀行、国家市場監督管理総局、国家ラジオテレビ総局、国家秘密保護局、国家暗号管理局、2020年6月1日施行）	対象：重要情報インフラ運営者 内容：重要情報インフラ運営者がネットワーク製品およびサービスを購入し、国家安全に影響を与え、または与えうる場合、国家安全審査に合格しなければならない。

(3) その他：推奨標準、産業別の関連法令

サイバーセキュリティおよびデータに関連する一般的な規制を示す基本法および法令のほか、特定の業界の特徴等を踏まえた法令も制定されています。例えば、自動車業界においては、「自動車データ安全管理規定（試行）」という法令があります。

また、サイバーセキュリティおよびデータに関しては、さまざまな推奨標準も公布されています。これらの推奨標準は強制力がないものの、法令および義務の履行、特に行政機関における認定および取り締まり等について理解する上で参考になります。

2. 法執行機関

サイバーセキュリティおよびデータに関連する法執行は、国レベルでは、国家インターネット情報弁公室、公安機関、国务院傘下のその他の機関により実施されています。具体的には以下のとおりです。

- (1) 国家インターネット情報機関は、ネットワーク・データセキュリティおよび関連監督管理業務の統括・調整の責任を負う（「サイバーセキュリティ法」第 8 条、「データセキュリティ法」第 6 条、「個人情報保護法」第 60 条等）。
- (2) 工業、電気通信、交通、金融、自然資源、衛生・健康、教育、科学技術等の主管機関は、各業界、各分野における監督管理の職責を負う。例えば、各業界における重要データリスト・重要情報インフラ運営者の確定、サイバーセキュリティ審査の実施（「データセキュリティ法」第 6 条、「個人情報保護法」第 60 条等）。
- (3) 公安機関、国家安全機関等は、各自の職責の範囲内において、サイバーセキュリティ・データセキュリティ監督管理の職責を負う（「サイバーセキュリティ法」第 8 条、「データセキュリティ法」第 6 条、「個人情報保護法」第 60 条等）。

3. 違法行為に対する法的責任

上述の法令では、違法行為について、以下のとおり、刑事上、行政上、民事上の責任を負うと定めています。

	主な違法行為	法的責任	法令名・条文番号
刑 事 責 任	営業秘密侵害罪	10 年以下の懲役、罰金の併科または単科	「刑法」第 219 条
	公民個人情報侵害罪	7 年以下の懲役、罰金の併科または単科	「刑法」第 253 条 その 1
	情報ネットワーク安全管理義務不履行罪	3 年以下の懲役、罰金の併科または単科	「刑法」第 286 条 その 1
行 政 責 任	データセキュリティ保護義務を履行しなかったこと	組織：200 万元以下の過料 責任者（個人）：20 万元以下の過料	「データセキュリティ法」第 45 条
	法律の規定に違反し、国外に重要データを提供したこと	組織：1,000 万元以下の過料 責任者（個人）：100 万元以下の過料	「データセキュリティ法」第 46 条
	法律の規定に違反する個人情報の取り扱い、または個人情報の取り扱いに必要な個人情報保護義務を履行しないこと	組織：違法所得の没収、5,000 万元以下または前年度の売上高の 5% 以下の過料 責任者（個人）：100 万元以下の過料	「個人情報保護法」第 66 条
民 事 責 任	個人情報の取り扱いにより個人情報に関する権益を侵害し、損害を与えたこと	個人情報取り扱い者：損害賠償等の権利侵害責任	「個人情報保護法」第 69 条

北京市環球法律事務所

レポートをご覧いただいた後、アンケート（所要時間：約1分）にご協力ください。

<https://www.jetro.go.jp/form5/pub/ora2/20210047>



本レポートに関するお問い合わせ先：
日本貿易振興機構（ジェトロ）
海外調査部 中国北アジア課
〒107-6006 東京都港区赤坂 1-12-32
TEL：03-3582-5181
E-mail：ORG@jetro.go.jp